US Department of Education
Federal Student Aid

START HERE
GO FURTHER
FEDERAL STUDENT AID

General Support System and Major Application Backup Media Handling Policy & Procedures

January 2007

Federal Student Aid CIO: IT Security 2-04 Page 1 of 10

Distribution: All Federal Student Aid Data Centers

Approved by: _____ 1/22/2007
Katie Blot, Federal Student Aid Chief Information Officer Date

Table of Contents

Document Revision History

This page summarizes the document revision history. Each entry includes the version number for the document itself, the date of the change, the page number(s) where the change occurred, and a (very) brief description of the change. The most current change will always appear on the first row of the table.

Any changes/updates to the document will be provided in detail in the Document Revision History table and will be distributed to the appropriate individuals. Revision bars on the left-hand side of the page will reflect the line(s) where a change has occurred. Complete the page number column only if minor changes are made. If the document is undergoing a complete revision, this field can be marked N/A.

Version	Date of Change	Page Number(s)	Brief Description of Change
1.0	2006-11-14	N/A	Development of Policy

1 OBJECTIVES

Backing up Federal Student Aid data on a secondary media is a common practice that provides Federal Student Aid the ability to transport, exchange, and recover critical data after a data loss has occurred. The objective of this policy is to increase the controls that are in place to protect the media while it is being moved within the Federal Student Aid facilities, contractor facilities, in transits and off-site. The increased controls will help Federal Student Aid identify and recover media that has been diverted from its intended destination.

2 SCOPE

This document applies to all General Support Systems and Major Applications, including those components operated by Federal Student Aid contractors. The policy addresses the handling and logging requirements for media backups used by General Support Systems and Major Applications.

This document is intended to supplement the Department of Educations Handbook OCIO-01, *Handbook for Information Assurance Policy*

3 POLICY

3.1 Labeling Backup Media

Labels must be affixed to all backup media indicating the media sensitivity level and a warning that only authorized personal may handle the physical media or access the stored information.

3.2 Data Encryption

All information stored on backup media must be encrypted using a NIST-approved encryption algorithm.

3.3 Storage of Data Backup Media

All backup media used to store data, operating system software, and application installation software, must be securely stored in an environmentally and physically protected facility geographically separate from the General Support Systems and Major Applications operations.

3.4 Access to Stored Backup Media

Access to all stored backup media must be restricted to authorized users with backup media responsibilities.

3.5 Backup Software Controls

Access to backup software must be restricted to user accounts with specific responsibilities for backup administration.

3.6 Auditing Backup Events

Backup event auditing and notification controls must be implemented.

3.7 Tracking Backup Media

General Support Systems and Major Applications must establish and maintain a c*hain of custody* record for each individual backup media while in storage at Federal Student Aid facilities, in transit to and from Federal Student Aid facilities, and while in storage at off-site facilities.

3.8 Backup Media Sanitization and Disposal

Backup media must be sanitized before reuse or disposal, using approved equipment, techniques, and procedures so that information recovery is not possible.

4 EXCEPTIONS

No portion of this policy can be waived. However, a business unit can maintain non-compliance with a portion of this policy if the business unit has made a risk based decision not to comply, and the Designated Approving Authority (DAA) approves that decision. The DAA for Federal Student Aid is its Chief Operating Officer.

Noncompliance with this policy shall be based on a business decision that:

- Other controls (technical or procedural) that limit the risk substantially enough to make the additional control required by this policy needless
- The risk the policy aims to minimize is already substantially remote
- The cost of implementing the policy is not commensurate with the protection offered by the policy
- The implementation of the policy will break or degrade system functionality
- The implementation of the policy will impose greater risks upon the system

A Department of Education Risk Analysis Form (RAF) must support each decision and clearly identify the following:

- Policy that is not being met
- Impact level
- Existing controls
- Threat level
- Likelihood of compromise
- Overall risk
- Justification for accepting the risk

Should a business decision be made to not comply with the policy, steps must be taken to reduce those risks to an acceptable level, update the System Security Plan, and maintain a satisfactory level of protection.

5 PROCEDURES

These procedures are based on *NIST SP 800-53* and industry best practices. *NIST SP 800-53* breaks down security controls into LOW, MODERATE and HIGH impacts based on the highest data sensitivity level. Additional controls for MODERATE and HIGH are identified after the general/LOW impact controls.

5.1 Labeling Backup Media

General Support Systems and Major Applications shall affix external labels to backup media in a manner that will not damage the stored data. Labels should be properly worded in a manner consistent with the following example:

```
U.S. Dept. Of ED Property
-SENSITIVE-
-FOR OFFICIAL USE ONLY-
Unauthorized possession or use
of this media is a violation of
Federal law.  If found, please
call XXX-XXX-XXXX
```

5.2 Data Encryption

Necessary controls will be applied to ensure that personally identifiable information and backup data is appropriately encrypted prior to being removed from any area under agency control and remains encrypted while in remote storage.

5.3 Storage of Backup Media

Data backup procedures must designate the location of stored data, media rotation frequency, and method for transporting data offsite.

MODERATE: A backup copy of the operating system and application software must be stored in a fire-rated container located within the Federal Student Aid facility, but not collocated with the operational software.

MODERATE: The alternate storage site is configured to facilitate timely and effective recovery operations.

MODERATE/HIGH: Business owners will ensure that media is physically controlled and securely stored.

HIGH: General Support Systems and Major Applications identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

5.4 Access to Stored Backup Media

Access to stored backup media must be restricted to personnel with backup responsibilities, including system backup administrators, backup media handles, and auditors. The system manager must designate the method of enforcement.

MODERATE/HIGH: Technical and automated control mechanisms are implemented to limit physical access and to audit access attempts and access granted.

MODERATE/HIGH: Video surveillance cameras are installed to act as a deterrent and to identify any improprieties that might occur.

5.5 Backup Software Access Controls

Separate operating system and backup administration accounts must be created for each individual user with responsibilities for both operating system administration and backup administration.

5.6 Auditing Backup Events

Technical mechanisms shall be implemented to track changes to backup software, schedules, and processes.

MODERATE: Event audit records shall be reviewed monthly to identify inconsistencies in backup events.

HIGH: Alerts are set to notify backup administrators of any deviations from normal backup processes and schedules.

5.7 Tracking Backup Media

Chain of custody records documenting the time, date, location, and persons handling backup media are maintained for each *point* in the *media storage and transit cycle*.

MODERATE: Auditing and tracking mechanisms are implemented that make immediate verification of the location and state of specific media possible both within Federal Student Aid facilities and while off-site.

MODERATE: Verification that individual backup media was received by off-site storage facility is reported to Federal Student Aid upon receipt.

MODERATE: Testing methods are implemented to verify the secure handling of backup media and information while off-site.

5.8 Backup Media Sanitization and Disposal

Sanitization includes removing all labels, markings, and activity logs. Sanitization techniques, such as degaussing and overwriting memory locations, must be implemented to ensure that Federal Student Aid information cannot be identified to unauthorized individuals when backup media is reused or disposed.

General Support Systems and Major Applications must track, document, and verify media sanitization actions and periodically tests sanitization equipment and procedures to ensure correct performance.

The National Security Agency maintains a list of approved products with degaussing capability at:

http://www.nsa.gov/ia/government/mdg.cfm

NIST Special Publication 800-36 provides guidance on appropriate sanitization equipment, techniques and procedures.

6 ROLES & RESPONSIBILITIES

6.1 Backup Administrators

Backup Administrators responsibilities include:

- Identifying and collecting backup media scheduled for transport to off-site storage facility.
- Ensuring that all data stored on backup media is properly encrypted
- Labeling backup media with sensitivity level and authorized use warning after creation.
- Maintaining the proper access control to backup media while local to Federal Student Aid facilities and awaiting transport to off-site facility.
- Ensuring that proper *chain of custody* documentation is maintained while backup media is located within Federal Student Aid facilities, and during transfer to off-site storage courier.
- Sanitizing backup media using approved methods before its disposal or release for reuse.

6.2 System Security Office / Project Manager

System Security Officer / Project Manager responsibilities include:

- Validating the proper implementation of access controls and documentation by third party contractors and off-site storage facilities.
- Verifying that Federal Student Aid backup media handling policies are consistently implemented at off-site media storage facilities.
- Ensuring that proper *chain of custody* documentation is consistently maintained throughout the *media storage and handling cycle*.
- Developing procedures and controls that address specific backup software, including configuration standards.
- Documenting the current process for secondary media backup procedures and environmental controls.
- Developing incident response plans or procedures for specific incidents such as accidents while transporting media, and handling events such as loss or theft, as they relate to individual General Support System and Major Application backup media storage processes.
- Ensuring access to backup media is restricted to authorized personnel.

7 INCIDENT RESPONSE TERMS & DEFINITION

Creating a ***chain of custody*** is a method of documenting the complete location and ownership history of media from the time of creation to its sanitation, whereby the location and owner of a particular media can be identified for any time and date during the transit and storage cycle. An item is considered to be in an individual's custody if the item is in the physical possession of that person or placed in a secured area or container by that person. Properly maintained Chain of Custody records can be used in the prosecution of unlawful acts.

A ***point of record*** is when the Chain of Custody documentation must be updated to reflect any change in the location or ownership of the media.

Sanitation of media refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be retrieved and reconstructed.

The ***media storage and transit cycle*** is the timeline of events from the initial point of backup media creation to the time of media sanitation. The cycle also includes each *point of record* where the location or ownership of backup media is changed.

8 ENFORCEMENT

Violation of this policy could result in loss of, or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

9 POINT OF CONTACT

Federal Student Aid Chief Security Officer (CSO)

10 ATTACHMENTS

11 AUTHORITY

- Federal Student Aid Information Technology Security and Privacy Policy
- Department of Education Handbook OCIO -01, *Handbook for Information Assurance Policy*
- Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

- OMB Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*, November 28, 2000.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*
- NIST Special Publication 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*
- NIST Special Publication 800-88, *Guidelines for Media Sanitation: Recommendations of the National Institute of Standards and Technology*
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost of Security in the Agency Information Technology Investments*

12 LOCATION

All Federal Student Aid security policies are located on the Online Security Center (OSC) at the following URL: http://thestartingline.ed.gov/cio/products/it_security_portal/policies/fsa.html

13 EFFECTIVE DATE

The effective date for this document is February 1, 2007.

14 REVIEW SCHEDULE

This document will be reviewed annually.